ABSTRACT OF THE DISCLOSURE

In a communication system wherein a device and a client communicate data with each other through a network, the device holds a root certificate including a public key in a pair of the public key and a private key and signed with the public key. When data is sent, a certificate creator creates a second certificate including the root certificate designated as a certificate authority at a higher level and signed with the root certificate, and the second certificate is sent to the client. In the client, the root certificate has been stored beforehand, and a verifier verifies the signature of the second certificate with the root certificate.